Handling Computer Security Incidents

Indian Computer Emergency Response Team

Ministry of Electronics and Information Technology
Government of India

सत्यमेव जयते

CERT-In Advisory CIAD-2016-0072

Online Payments through Unified Payment Interface

Original Issue Date: December 08, 2016

Description

Unified Payment Interface (UPI) is an initiative by National Payments Corporation of India (NPCI), set up with the support of the Reserve Bank of India with a vision of migrating towards a "less-cash" and more digital society.

UPI is a system that enables peer to peer online payments for users holding different bank accounts, to send and receive money or to pay directly to merchants from their Smartphone without the need to enter bank account information or net banking UserID / Password.

UPI has built on the Immediate Payment Service (IMPS) platform.

How it works

For using Unified Payment Interface, users need to create a Virtual ID or Virtual Payment Address (VPA) of their choice to link it to any bank account. This process doesn't require either the payee or payer to share bank details. The VPA acts as their financial address and users need not remember beneficiary account number, IFSC codes or net banking user id/password for sending or receiving money.

1. Registration

Steps for Registration:

- User downloads the Unified Payment Interface application from the App Store / Banks website.
- User creates his/ her profile by entering details like name, virtual id (payment address), password etc.
- User goes to "Add/Link/Manage Bank Account" option and links the bank and account number with the virtual id.

Generating M-PIN:

- User selects the bank account from which he/she wants to initiate the transaction.
- User clicks on the given options as required.

2. Performing a Unified Payment Interface Transaction

PUSH-sending money using virtual address

- User logs in to UPI application.
- After successful login, user selects the option of Send Money / Payment.
- User enters beneficiary's / Payee virtual id, amount and selects account to be debited.
- User gets confirmation screen to review the payment details and clicks on Confirm.
- User now enters MPIN.
- User gets successful or failure message.

PULL-Requesting money

- User logs in to his bank's UPI application.
- After successful login, user selects the option of collect money (request for payment).
- User enters remitters / payers virtual id, amount and account to be credited.
- User gets confirmation screen to review the payment details and clicks on confirm.
- The payer will get the notification on his mobile for request money.
- Payer now clicks on the notification and opens his banks UPI app where he reviews payment request.
- Payer then decides to click on accept or decline.
- In case of accept payment, payer will enter MPIN to authorize the transaction.
- Transaction complete, payer gets successful or decline transaction notification.
- Payee / requester get notification and SMS from bank for credit of his bank account.

Advantages

- With UPI, user's bank account can be used as a wallet with a simplified two-factor authentication which eliminates the need to store funds in any other wallet.
- Use of Virtual ID makes it more secure since there is no need to share credentials.
- UPI transaction can be made via IMPS in real time, which makes it available 24*7.
- Users can link multiple bank accounts to a single Smartphone. Hence sending or receiving money across banks is easier.
- For merchants, it is Suitable for electronic Commerce and a mobile Commerce transaction as well as it resolves the Cash on Delivery collection problem.
- Banks can create their own application interfaces as UPI provides flexibility and an open architecture.

Security Measures

- Beware of Mobile phishing: always download legitimate UPI applications from bank's official website, and be cautious before you download it from App store.
- Keep strong passwords for your phone as well as for your UPI application.
- Do not share MPIN with anybody (not even with bank), and be suspicious of unknown callers claiming to be from your bank.
- Use biometric authentication if possible.
- Update your mobile OS and applications as often as possible to be secure from vulnerabilities.
- It is advisable for users to enable encryption, remote wipe abilities and anti-virus software on the phone.
- Keep your SIM card locked with a Pin to avoid misuse, in case of loss or theft of the mobile device, You can contact your subscriber to block the subscription of the SIM card.
- Avoid connecting phones to unsecured wireless networks that do not need passwords to access.

References

NCPI
http://www.npci.org.in/UPI_Background.aspx
http://www.npci.org.in/documents/UPI-Linking-Specs-ver-1.1_draft.pdf

CERT-In
Safeguarding Smart phones against Cyber attacks (CIAD-2016-0069)
http://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2016-0069

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email: info@cert-in.org.in
Phone: +91-11-24368572

Postal address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India